

## IN THE CLAIMS

1-12. (Cancelled)

13. (Currently Amended) A method of assessing a risk of a terrorist attack on a site comprising the steps of:

calculating a probability that a terrorist attack on the site ~~an event~~ will occur;

calculating a vulnerability to the terrorist attack on the site, the vulnerability being based on a susceptibility to the terrorist attack and a consequence of the terrorist attack, the susceptibility being based on an accessibility determined from a model of the physical environment of the site [[event]]; and

calculating a relative risk based on the probability and vulnerability;

wherein the calculating steps are performed using an artificial intelligence network.

14. (Previously Presented) The method of Claim 13, wherein the artificial intelligence network is a Bayesian network.

15-41. (Cancelled)

42. (New) The method of claim 13, wherein the accessibility is determined for a weapon, delivery system and specific target at the site chosen by a user.

43. (New) The method of claim 42, wherein a plurality of approach vectors are determined for delivery of the weapon by the delivery system to the specific target at the site.

44. (New) The method of claim 43, wherein countermeasures along the approach vectors are evaluated and the approach vectors are modified in response to the countermeasures where necessary.

45. (New) The method of claim 13, further comprising the step of modifying the physical model of the site to add at least one additional countermeasure and re-calculating the accessibility for the modified physical model.